HW 05 CMSC/MATH/ENEE 456. Morally DUE Oct 19
WARNING: THE HW IS 12 PAGES LONG
(Its not Long, I have made one-problem-per-page)

1. (0 points)

   (a) What is the day and time of the timed part of the midterm?

   (b) IF you CANNOT make the timed part of the midterm let me know NOW!!!!!!!!!!

   ADVICE for this HW: You might want to use

   - Wolfram Alpha
   - This website: `https://planetcalc.com/3311/`

GOTO NEXT PAGE

2. (30 points) In this problem Alice and Bob are doing Diffie Hellman with $p = 31$ and $g = 2$. Note that g is NOT a generator.

   (a) (20 points) Alice uses $a = 8$ and Bob uses $b = 9$. What is the shared secret key? Express as a number in $\{0, \ldots, 30\}$

GOTO NEXT PAGE

(b) (10 points) Note that Alice and Bob used a NON-generator for g but they were still able to establish a shared secret key. Why is using a non-generator a bad idea? Use the example of $p = 31$ and $g = 2$ to make your point. (No hints or help will be given on this- I want you to think about it!)

GOTO NEXT PAGE

3. (30 points) In this problem Alice and Bob are doing Diffie Hellman with $p = 47$ and $g = 5$. Note that g IS a generator.

   (a) (5 points) Alice uses $a = 10$ and Bob uses $b = 11$. What is the shared secret key? Express as a number in $\{0, \ldots, 46\}$

GOTO NEXT PAGE

(b) (5 points) Alice uses $a = 11$ and Bob uses $b = 10$. What is the shared secret key? Express as a number in $\{0, \ldots, 46\}$

GOTO NEXT PAGE

(c) (20 points) If you did the problem correctly the last two answers were the same. Prove the following theorem:

Theorem Let p be a prime and g be a generator. Let $a, b \in \{0, \ldots, p-1\}$. Let $s_{a,b}$ be the shared secret key if Alice uses a and Bob uses b. Show that $s_{a,b} = s_{b,a}$.

GOTO NEXT PAGE

4. (20 points) Alice and Bob are going to use RSA with primes $p = 7$ and $q = 11$.

   (a) (10 points) List all possible values of $e \geq 10$ that Alice could pick. (In real life we demand that e be between $R/3$ and $2R/3$. For this problem, and for all HW, we drop that demand since we are dealing with small numbers and toy examples. For THIS problem I DO insist that $e \geq 10$.)

GOTO NEXT PAGE

(b) (10 points) Let e be a number NOT on the list in the last item. What goes wrong if Alice tries to use e?

GOTO NEXT PAGE

5. (20 point) Alice and Bob are again using RSA with $p = 7$ and $q = 11$. Let $e = 13$ (This is a value that can be used).

   (a) (5 points) What is d?

GOTO NEXT PAGE

(b) (5 points) What does Alice broadcast? What does she keep secret?

GOTO NEXT PAGE

(c) (5 points) Bob wants to send 30. What does he send?

GOTO NEXT PAGE

(d) (5 points) To send m Bob sends 71. Show how Alice determines m and also give us m.